



UNIVERSITI SAINS ISLAM MALAYSIA

جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

DECLARATION OF THESIS/ UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's Full Name:

LUQMANUL HAKIM BN MOHD NASIR

Student's Number:

3060007

Title:

SECURED AUTONOMOUS AGENT-BASED
INTRUSION DETECTION SYSTEM
(SAIDS)

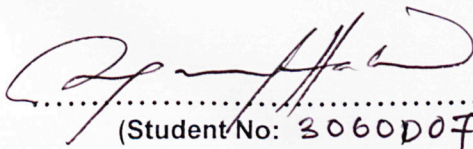
Academic Session:

2 2010 / 2011

I hereby declare that the work in this thesis/ project paper is my own except for quotations and summaries which have been duly acknowledged.

I acknowledged that Universiti Sains Islam Malaysia reserves the right as follows:

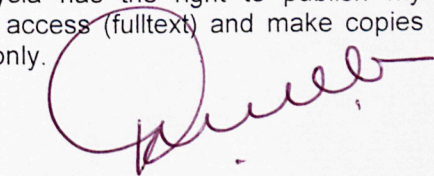
1. The thesis/ undergraduate project paper is the property of Universiti Sains Islam Malaysia.
2. The library of Universiti Sains Islam Malaysia has the right to publish my thesis/ undergraduate project paper as online open access (fulltext) and make copies for the purpose of research or teaching and learning only.


.....
(Student No: 3060007)

(Pasport No: J21014-04-5065)

Date:

8/3/2011


.....

(Signature of Supervisor)

PROF. DR. KAMARUZAMAN
BIN JEMAN

Date:

8/3/2011

**SECURED AUTONOMOUS AGENT-BASED
INTRUSION DETECTION SYSTEM (SAAIDS)**

LuqmanulHakim Bin Mohd Nasir
(Matric No. 3060007)

Thesis submitted in fulfillment for the degree of
MASTER OF SCIENCE

Faculty of Science and Technology
UNIVERSITI SAINS ISLAM MALAYSIA
NILAI

March 2011

AUTHOR DECLARATION

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 4th March 2011

Signature: 

Name: LuqmanulHakim Bin Mohd Nasir

Matric No: 3060007

Address: No. 2, Lot 14776,
Jalan Sungai Sekamat,
Bt. 12 ½, Jalan Cheras,
43000 Kajang,
Selangor Darul Ehsan.

LuqmanulHakim Bin Mohd Nasir (3060007) was born on the 14th October 1982. He is currently residing at No. 2, Lot 14776, Jalan Sungai Sekamat, Bt. 12 ½, Jalan Cheras, 43000 Kajang, Selangor Darul Ehsan. He previously was a student of UTM and obtained Bachelor of Computer Science from Faculty of Computer Science and Information System. He is at present a Master student of USIM majoring in Information Security.

ACKNOWLEDGEMENT

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Praise be upon Allah the Most Gracious Most Merciful for His blessings to enable this completion of research project thesis.

My gratitude goes to my supervisor, Prof. Dr. Kamaruzzaman Seman and my co-supervisor Mrs. Madihah Mohd Saudi for their high dedication, useful guidance and invaluable advices along my research.

I would like to thank Universiti Sains Islam Malaysia (USIM) administration for giving me chances to gain knowledge and experience along my study period. Thanks to Ministry of Science, Technology and Innovation (MOSTI) for their scholarship and grant in ensuring this research is done.

I am most grateful to my parents, Mr. Hj. Mohd Nasir and Mrs. Hjh. Fauziah and my family members for their unlimited prays, love and support. To my beloved wife, Juraida Asna Marhaban and my beloved daughter, Damia Mardhiah for their love, patience and always being there for me. Last but not least, thanks to all my friends and colleagues in USIM and UTM for their unforgotten helps, invaluable guidance, fruitful discussions and ideas about this project.

Thank you.

ABSTRACT

Secured Autonomous Agent-Based Intrusion Detection System (SAAIDS) is developed to design new agent-based intrusion detection system (IDS) based on newly designed SAAIDS architecture and design agent communication and verification protocols and algorithms. The architecture tends to provide secure agent communication and protection of the agent itself. In overcoming problems in existing agent-based IDS, the architecture of SAAIDS is designed to enrol all components in an agent. P2P connection solved single point of failure, multilevel authorization problem and delay on information sending by its design which provides direct connection between agents. In avoiding attacks on message sending process, the architecture was designed with agent communication protocol and algorithm tends to provide secured communication between agents. Agent Verification Protocol and algorithm designed to avoid from unauthorized agent running and doing damages in the system. The unauthorized agent produced when agents being duplicated or altered. The newly designed architecture of SAAIDS, Agent Communication and Verification Protocol and Algorithm was developed and implemented. At the end of the research phase, system testing has proved that the proposed solutions able to avoid all the problems stated above.

LIST OF TABLES

	Page
Table 3.1: UML and Components	52
Table 3.2: Use Case Login Description	57
Table 3.3: Use Case Control Agents Description	58
Table 3.4: Use Case View Logs Description	58
Table 4.1: Snort Default Classification	82
Table 4.2: Agent's Attribute	85
Table 4.3: MYSQL Data Type and Format for DATETIME, DATE, TIME and TIMESTAMP	86
Table 4.4: Message Priority	91
Table 6.1: Unit Testing for Administrator Module	121
Table 6.2: Unit Testing for Agent Communication Module	122
Table 6.3: Unit Testing for Agent Verification Module	123
Table 6.4: Unit Testing for Agent Response Module	124

LIST OF FIGURES

	Page
Figure 1.1: Research Activity Flowchart	6
Figure 2.1: Incident Statistics for 2006	15
Figure 2.2: Attacks Classification	16
Figure 2.3: Attacks Classification	19
Figure 2.4: Fundamental of IDS	20
Figure 2.5: An Overview of Classification of Intrusion Detection System	22
Figure 2.6: Centralized Control Strategy	27
Figure 2.7: Partially Distributed Control Strategy	27
Figure 2.8: Fully Distributed Control Strategy	28
Figure 2.9: Public Key System Concept	37
Figure 2.10: SHA1 with Elgamal Digital Signature	39
Figure 2.11: AAFID Overview	40
Figure 2.12: PAID Overview	41
Figure 2.13: IDA Overview	42
Figure 3.1: Prototype Paradigm	50
Figure 3.2: Administrator Use Case Diagram	57
Figure 3.3: Administrator Activity Diagram	59
Figure 3.4: Intrusion Detection Activity Diagram	60
Figure 3.5: Agent Communication Activity Diagram	61
Figure 3.6: Agent Verification Activity Diagram	63
Figure 3.7: Controlling Agents Sequence Diagram	65
Figure 3.8: Viewing Logs Sequence Diagram	66
Figure 3.9: Intrusion Detection Sequence Diagram	66
Figure 3.10: Agent Communication Sequence Diagram	67
Figure 3.11: Agent Verification Sequence Diagram	68
Figure 3.12: System Package Diagram	69
Figure 3.13: Subpackages in Detection Package	69
Figure 3.14: Subpackages in Monitor Package	70
Figure 3.15: Subpackages in Transceiver Package	70
Figure 3.16: Subpackages in Security Package	71

Figure 3.17: SAAIDS Class Diagram	72
Figure 3.18: Entity Relationship Diagram	73
Figure 3.19: Data Environment Designer	74
Figure 4.1: SAAIDS Architecture	77
Figure 4.2: Agent Communication Protocol	87
Figure 4.3: P2P Connection	88
Figure 4.4: Overview of Elgamal Encryption	90
Figure 4.5: Agent Communication Algorithm	93
Figure 4.6: Agent Verification Protocol	95
Figure 4.7: Overview of Elgamal Digital Signature	97
Figure 4.8: SHA1 with Elgamal Digital Signature	98
Figure 4.9: New and Existing Agent Verification	98
Figure 4.10: Agent Verification Algorithm	102
Figure 5.1: System Modules	105
Figure 5.2: Administrator Modules Coding	106
Figure 5.3: Login Interface	107
Figure 5.4: Error Login Message Interface	107
Figure 5.5: Agent Communication Module Coding	108
Figure 5.6: Detection Response Module Interface	109
Figure 5.7: Agent Verification Module Coding	110
Figure 5.8: Verification Response Module Interface	111
Figure 6.1: Path Graph for Login Procedure	114
Figure 6.2: Path Graph for Receive Message Procedure	115
Figure 6.3: Path Graph for Encrypt and Decrypt Procedure	116
Figure 6.4: Path Graph for Verifier and Verified Procedure	117
Figure 6.5: Path Graph for Response Module Procedure	118
Figure 6.6: Testing Event 1	126
Figure 6.7: Testing Event 2	127
Figure 6.8: Testing Event 3	128
Figure 6.9: Result for Testing Event 1	128
Figure 6.10: Result for Testing Event 2	129
Figure 6.11: Result for Testing Event 3	130

TABLE OF CONTENTS

CONTENTS	PAGE
AUTHOR DECLARATION	i
BIODATA OF AUTHOR	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
LIST OF TABLES	v
LIST OF FIGURES	vi
TABLE OF CONTENTS	viii
LIST OF APPENDICES	ix
CHAPTER I: INTRODUCTION	1
CHAPTER II: LITERATURE REVIEW	13
CHAPTER III: SYSTEM METHODOLOGY	49
CHAPTER IV: SYSTEM ARCHITECTURE AND DESIGN	75
CHAPTER V: SYSTEM IMPLEMENTATION	104
CHAPTER VI: SYSTEM TESTING	112
CHAPTER VII: CONCLUSION AND FUTURE WORK	127
BIBLIOGRAPHY	140
APPENDICES	143

LIST OF APPENDICES

	Page
Appendix A: Project Time Schedule	143